DOCUPHASE

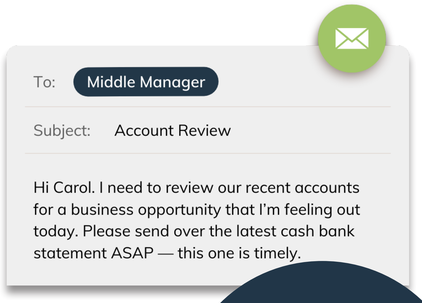
Hook, Line, and Sinking Financials:

A DEEP DIVE INTO PHISHING ATTACKS ON AP TEAMS & EXECS

PHISHING: Emails, texts or calls that appear to come from a known source or reputable company in order to convince targets to reveal personal or sensitive information.

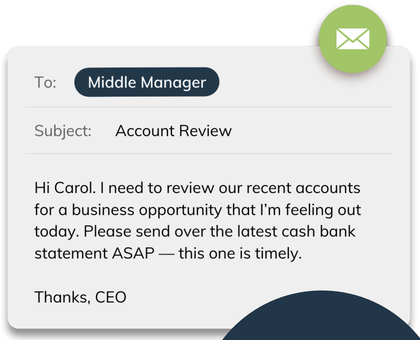
AP DEPARTMENT

AP is the most susceptible department to Business Email Compromise (BEC).[2] Fraudsters mimic vendors to request payments, and send fake invoices that infiltrate company AP systems when opened.



Always call to verify an invoice or requested changes in payment instructions before making a payment. Implement a two-step verification process for all payments.

58% of AFP survey respondents were compromised through email scams in 2022.[3]



40% of middle managers click on an email the day it's sent.[2]

MIDDLE MANAGERS

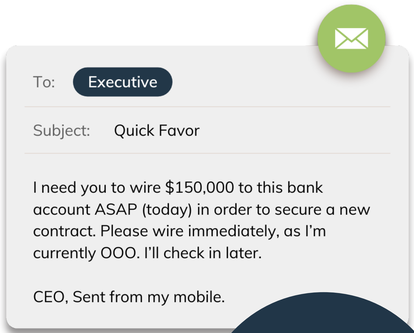
Fraudsters exploit busy, multitasking managers who are under a lot of pressure, are inundated with a high volume of emails and are expected to respond quickly — especially to executives.

Verify all email requests for sensitive information over a different communication channel.

C-SUITE

(AKA "Whaling," "CEO Fraud" and "Executive Phishing.")

These high-value targets have access to sensitive data like financial accounts and employee W-2 info. Fraudsters steal login details to "spoof" their account and send emails "from" execs.



Train executives on phishing threats, and use multi-factor authentication for all financial transfers.

96% of executives are vulnerable to phishing attacks.[1]

74% of data breaches in 2022 involved the human element.[4]

Move your workflow out of your inbox and into a secure, centralized system to minimize your risk of BEC. 60% of DocuPhase customers said that the platform reduces emails thanks to built-in workflow and collaboration tools.

Ready to level up your security?

GET A DEMO

DocuPhase | 13577 Feather Sound Drive, Clearwater, FL 33762 | info@docuphase.com | www.docuphase.com